METHOD AND APPARATUS FOR CONTENT-BASED INTRUSION DETECTION USING AN AGILE KERNEL-BASED AUDITOR

ABSTRACT

One embodiment of the present invention provides content-based intrusion detection for a computer system by using an agile kernel-based auditing system. This auditing system operates by receiving an audit specification that specifies target attributes to be recorded during an auditing process. The audit specification also specifies an auditing criterion that triggers recording of the target attributes. Upon receiving the audit specification, the auditing system is configured to record the target attributes during system calls whenever the auditing criterion is satisfied. Next, an application program is monitored by the auditing system to produce an audit log containing the recorded target attributes. This audit log is examined in order to detect patterns for intrusion detection purposes. In one embodiment of the present invention, configuring the auditing system involves compiling the audit specification to produce a kernel module, and then loading the kernel module into a kernel of an operating system. It also involves linking code from within the kernel module into system calls within the operating system. In one embodiment of the present invention, in response to detecting an event during the auditing process, the system dynamically adjusts the auditing system to change the auditing criterion and/or the target attributes for subsequent operation of the auditing system.